# Program Protection Planning in the USAF TENCAP Program: A Real-World Application of Risk Management to Contain Security Costs©

Session: Technical and Policy Focus Groups

Howard B. Low
Aegis Research Corporation
Space Engineering Center
1551 Vapor Trail
Colorado Springs, CO 80916
(719) 570-7041/567-9946
Fax (719) 570-7689/567-9898
E-mail: lowhowab@fafb.af.mil, hblow@pcisys.net

## Program Protection Planning in the USAF TENCAP Program: A Real-World Application of Risk Management to Contain Security Costs©

Good morning. I am Bruce Low, from Aegis Research Corporation.

My topic this morning is a review of how the Air Force Material Command's (AFMC) Space and Missile System Center (SMC) Space Applications Project Office (SAPO) acquisition security organization supports the USAF Tactical Exploitation of National Capabilities (TENCAP) program. I will be focusing on how we apply the principles of risk management to acquisition security in order to contain security costs.

Acquisition security underwent a major change in the early 1990's when the Department of Defense (DoD) moved from strict risk avoidance to tailored risk management as the basis for program protection planning and system security engineering. Program Executives no longer had to follow a set of inflexible guidelines that had little relationship to the threat; they could now actively manage their security programs based on specific threats.

Evolving methodologies and subroutines have allowed increasingly credible risk acceptance decisions as the security risk management approach has matured. Focusing on the highest threats while accepting residual risks translates into successfully targeting security investments to when and where they are the most effective.

The impact of this change on the Air Force has been far reaching, extending from major acquisition programs to smaller projects, like proofs of concept, technology demonstrations, and rapid prototyping. Today's talk focuses on the USAF TENCAP program as an excellent example of applying the security risk management approach to a family of smaller projects within individual TENCAP TALON programs.

-----

Air Force Policy Directives and Instructions do not specify a methodology to achieve risk management goals, allowing senior Program Executives to choose government and industry 'best practices' to reach the desired program protection outcome within specific budget constraints. The SAPO, as the USAF TENCAP acquisition lead, chose a series of proven subroutines from other SMC programs to implement this DOD and USAF risk management direction.

These subroutines respond to these questions:

- *What must be protected?* The SAPO uses a standardized working aid (based on DOD, USAF and SMC classification guidelines for military space-related programs) to identify individual facts needing protection. These guidelines define what 'critical program information' (CPI) require protection as data that, if compromised, would significantly alter program direction; compromise program or system capabilities; shorten the expected combat-effective life of the system; or require additional research, development, test, and evaluation resources to counter the impact of CPI compromise. We look at the following areas:
  - Does the activity provide the U.S with a scientific, technical, operational, intelligence or battlefield advantage?
  - Is there reason to believe knowledge of the activity would allow a foreign nation to develop, improve or refine a similar item, or develop countermeasures?

- Does the activity provide information that would reduce or erode U.S. space dominance through denial of access to space in peace or war; reveal operational space doctrine; or, provide information on DOD reliance on civil or commercial space systems in crisis?

• *Why are the CPI protected?* We apply interim classification levels under Executive Order (E.O.) 12958 guidelines to protect CPI identified in the '*what*' step based on the information's criticality to either the U.S. or potential military and economic adversaries. Criticality analyses from the U.S. perspective address how the activity relates to mission requirements and capabilities; what opportunity does the activity provide to achieve technical or strategic surprise; what are the political impacts; and, what vulnerabilities are revealed? Criticality from an adversaries perspective addresses if the information allows them the opportunity to duplicate or counter the activity?

Depending on the responses to these questions, final classification levels assigned by an Original Classification Authority, as defined by the E.O. are:

- Top Secret - information that, if compromised, could cause 'exceptionally grave damage'.
- Secret - information that, if compromised, could cause 'serious damage'.
- Confidential - information that, if compromised, could cause 'damage'.

Another set of data that does not fall under the E.O. for formal classification, but is protected by the Government under contract law, are the USAF TENCAP contractor teams' proprietary data and trade secrets. Maintaining the privacy of this data, focusing on commercial information and products with particular interest in dual-use technologies, is essential to maintaining the health and competitiveness of this team.

• *Who is the CPI protected from?* The DoD assigns responsibilities for threat analysis support to individual national and military department security, intelligence, and counterintelligence (CI) activities. The resulting studies are published at varying levels of detail and classification, such as the unclassified National CounterIntelligence Center's *Annual Report to Congress on Foreign Economic Collection and Industrial Espionage,* supplemented by classified notes. This report has recently reaffirmed that at least 23 countries continue both commercially sponsored and foreign intelligence service intelligence collection against government and commercial targets in the U.S.

The USAF TENCAP risk management team refines this general threat to the nation's secrets and tailors our security countermeasures to defeat collection activities of specific threats against USAF TENCAP activities and sites. This tailored threat response, provided by the implementing command, is detailed in the Program Protection Plan (PPP), which then steps through the remainder of the methodology to identify security costs, related benefits and residual risks. The USAF TENCAP Director has this information available as he makes decisions about security and CI countermeasures used to defeat specific threats to his projects. This is exactly the type of cost containment outcome envisioned by using a focused threat for the risk management process.

*Program* protection analyses are separate from *system* security engineering analyses reported in the System Security Management Plan (SSMP). The program protection analysis describe security activities supporting the total development environment. The SSMP looks at threats to each system, assessing what an adversary might be able to do to defeat or interfere with our system.

An example of one of the savings we have been able to affect in USAF TENCAP projects comes from avoiding duplication in developing the threat baseline for computer systems by using the conclusions of the 'software risk assessment' developed for Certification and Accreditation (C&A) by the Designated Approval Authority (DAA) as the threat for the PPP and SSMP.

Many TENCAP projects have focused on enhancing the processing and delivery of data to the warfighter through automated information systems – hardware, firmware and software – using either commercial or government off-the-shelf (COTS/GOTS) products whenever possible. Current USAF rules for the development of computer systems, even if unclassified, requires that we perform a risk assessment concerning these systems. Because we operate within an TS/SCI environment, we focus on the remaining HUMINT threat of the possibility that malicious logic might have been inserted into the COTS/GOTS software that forms the baseline for many of these projects. We do this through a modified software risk assessment that reviews the development history of the software by providing an audit trail of the people involved, as well as a review of the security status of facilities and platforms used. Not only does this software risk assessment support risk acceptance decisions by the USAF TENCAP Program Executive for program protection planning and system security engineering, it is also a major part of the C&A package submitted to the DAA.

These classified programs are relatively easy to assess. Software programmers and integrators already have active security clearances (e.g., they are in a trusted relationship with the Government based on various background checks), and the work is performed in a secure environment (the developmental computer system is protected from unauthorized physical and electronic access). Even though not required, most unclassified programs use the same cleared individuals in the same secure facilities used for classified programs. (There are management advantages to the contractor, Lockheed Martin Missile Systems, and it simplifies the Government's risk assessment process.)

COTS/GOTS software packages bring their own history with them, as well. Even though the Government may not be able to get a complete development history, with known personnel and access risks, the fact that the software has been developed by a major supplier and/or has been running virus-free for a period of time (especially in a classified mode at another Government location), reduces the risks that the Government accepts as part of the Program.

In the best case the software has been developed by individuals holding Government clearances on a system that has both physical and software security controls. In this case, the decision is very straightforward.

In less clear situations, the developers may be unknown, may be employees of a foreign company, be foreign national employees of a U.S. company, or simply be U.S. citizens who do not hold a security clearance. Higher risk scenarios might also include employees with a history of some activity that qualifies them for their company's Employee Assistance Program. Also, the development platform may have been located in an uncontrolled area where anyone could have had access to it, had dial-up access, or been able to access it via an Internet connection.

In this example, all of this information, summarized and weighted for both the C&A DAA and USAF TENCAP Program Executive, allows reasoned risk acceptance decisions on multiple fronts using the same data, saving time and money.

- *When and where can the CPI be protected?* During this step we perform 'exposure analyses' for critical and sensitive data, describing the full range of candidate countermeasures that could reduce the threats to both the *program* and the *system*. The analyst puts himself into the position of a hostile force, knowing the entire range of intelligence sources and methods available to that planner, and studies where CPI might be collected. *Program* protection countermeasures to this collection, as recommended in the Program Protection Plan (PPP), will clearly be security oriented, including such things as production line controls to account for classified hardware, OPSEC during testing and evaluation, enhancements to facility security to control personnel access, etc. On the other hand, *system* countermeasures reported through the SSMP might respond to a wide variety of technical susceptibilities. These also include some that are purely security, such as RTIC/RTOC (Real Time Information into the Cockpit/Real Time Out of the Cockpit) software features that defeat spoofing and encryption to nullify hostile intercepts of sensitive data, but could also include such things as system design features to counter jamming, hardening against soft kill mechanisms, etc.

- *How can the CPI best be protected?* Working together, acquisition, security, intelligence, and CI organizations recommend security and operations risk management options for the CPI from the broad range of candidates. Within the USAF TENCAP world, threat exposure analyses have led to a small number of specific countermeasure recommendations supplementing the TS/SCI environment, most of them fairly straightforward. For example, in the AIS discussion we had earlier, the greatest 'exposure' occurred during software development when it was most likely that malicious logic might be inserted into the code. The response was limiting physical and electronic access to the code to individual programmers who are in a 'trusted relationship' with the Government. Another example is encrypting data transmissions that contain sensitive test results that can be overheard by hostile intercept.

We provide the AFTENCAP Program Executive our best estimate of the costs and benefits of each security risk management option. These 'costs' may be direct (dollars), or indirect (negative schedule impact, reduced operational capability, etc.). In each case the decision brief clearly identifies the residual risks assumed by the Program Executive as a result of these risk acceptance decisions.

Quality control during implementation is critical to the success of the process – poorly executed program protection and system security management plans are not only a waste of money, the resulting false sense of security will significantly increase the risk of losing the information you most want to protect. Contractor activities taking place at a contractor location are supervised under the DD254, Contract Security Classification Specification. Government activities taking place at Government locations are controlled and monitored by Government members of the project Integrated Product Team (IPT), or under specific project Memoranda or Agreement (MOA).

To insure that the analyses and recommendations forming the basis for the Program Executives' residual risk decisions remain valid in the face of evolving government-sponsored and commercial threats, the Program Security Manager monitors and fine tunes the countermeasures package during implementation. This requires good CI feedback, as well as the use of other data management tools measuring the exposure of sensitive information.

-----

AFMC, through the SAPO, has proven that this security risk management methodology, used elsewhere on larger space programs, is equally valid for fast moving smaller tasks (like the TENCAP Program's TALON projects). We continue to refine the process, applying the lessons we've learned to improve efficiencies and provide continuing successful program protection and system security engineering in the face of declining budgets. As a result of our extensive experience with this set of subroutines, we believe that this methodology can be applied anywhere in the DoD. It works equally well on programs with widely varying budgets and schedules. With modifications to accomodate minor variances in departmental guidelines, it can satisfy requirements is other USG Departments. It can even be successfully applied in the commercial world. We invite you to consider it to address your future needs.

- END -

## References

1. Economic Espionage Act of 1996, Title 18 U.S.C. 1831 et. seq.
2. Executive Order 12958, Classified National Security Information, 20 Apr 1995.
3. DoD 5000.2-R, Mandatory Procedures for Major Defense Acquisition Programs (MDAPs) and Major Automated Information System (MAIS) Acquisition Programs, (Includes Change 2), 06 Oct 1997.
4. DoD Directive 5200.39, Security, Intelligence, and Counterintelligence Support to Acquisition Program Protection, 10 Sep 1997.
5. DOD 5200.1-M, Acquisition Systems Protection Program, 16 Mar 1994.
6. DoD 5200.1-R, DoD Information Security Program, Jan 1997.
7. Draft DOD Directive 3500.2, Space Systems Protect Program, 22 Aug 96.
8. ASPWG PH-1, Acquisition Systems Protection Program Workbook, Sep 1994
9. Air Force Policy Directive 31-7, Security, Acquisition Security, 02 Mar 1993.
10. AF Policy Directive 31- 4, Information Security, 01 Aug 1997
11. AF Instruction 31-401, Managing the Information Security Program, 22 Jul 1994
12. Air Force Instruction 31-701, Security, Program Protection Planning, 18 Feb 1994.
13. Air Force Instruction 31-702, Security, System Security Engineering, 18 Feb 1994.
14. Air Force TENCAP Program Management Directive, PMD TEN 1 (02)/PE#27247F, 13 Sep 95.
15. AF TENCAP Program Plan FY98, 01 Aug 1997.
16. Space Warfare Center AFTENCAP Project Process Handbook, Jun 1997.
17. Air Force Space Command/Space Warfare Center/Air Force TENCAP Transition Guide, (Draft) 01 Apr 1997.
18. Space Applications Project Office/Space Warfare Center, AFTENCAP Project Security Checklist, 30 Jan 1998.
19. Space Applications Project Office/Space Warfare Center, Project Plan Security Working Aid – 1, Project Protection Plan Outline, 30 Jan 1998.
20. Space Applications Project Office/Space Warfare Center, Project Plan Security Working Aid – 2, Data List, 30 Jan 1998.
21. Space Applications Project Office/Space Warfare Center, Project Plan Security Working Aid – 3, Project Security Strategy, 30 Jan 1998.
22. Space Applications Project Office/Space Warfare Center, Project Plan Security Working Aid – 4, Preliminary System Security Management Plan, 30 Jan 1998.
23. Space Applications Project Office/Space Warfare Center, Project Plan Security Working Aid – 5, Project Threat Survey, 30 Jan 1998.